UDC 004.056.55
Doi: 10.31772/2587-6066-2019-20-1-20-27

For citation: Merinov A. S., Nesterov K. A., Zhdanov O. N. [Improvement of the construction technique of substitution blocks for symmetric encryption algorithms]. *Siberian Journal of Science and Technology.* 2019, Vol. 20, No. 1, P. 20–27. Doi: 10.31772/2587-6066-2019-20-1-20-27

Для цитирования: Меринов А. С., Нестеров К. А., Жданов О. Н. Совершенствование методики конструирования блоков замен для алгоритмов симметричного шифрования // Сибирский журнал науки и технологий. 2019. Т. 20, № 1. С. 20–27. Doi: 10.31772/2587-6066-2019-20-1-20-27

IMPROVEMENT OF THE CONSTRUCTION TECHNIQUE OF SUBSTITUTION BLOCKS FOR SYMMETRIC ENCRYPTION ALGORITHMS

A. S. Merinov, K. A. Nesterov, O. N. Zhdanov*

Reshetnev Siberian State University of Science and Technology
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russian Federation
*E-mail: onzhdanov@mail.ru

As it is known, block symmetric encryption algorithms are widely used to ensure information confidentiality. The resistance of encryption algorithms to the most common types of cryptanalysis is determined the quality of the blocks of substitutions.

In the present work, the development of a methodology for constructing substitution blocks is being continued.

In the first approach, Boolean functions with given cryptographic properties are used as component functions of substitution blocks. Previously, one of the authors proposed a reasonable methodology for the phased selection of Boolean functions for construction block.

In this paper, in addition to such cryptographic properties of Boolean functions, such as: balance, possessing a strict avalanche effect, possessing correlation immunity, for the first time the nonlinearity distances of the first and second orders of Boolean functions are considered simultaneously.

A study of the full set of Boolean functions of four variables was conducted. The result of it is the optimal set of Boolean functions for building substitution blocks when encrypted with the GOST 28147-89 algorithm.

In the second approach, the substitution block are determined by an irreducible polynomial over the Galois field, such a scheme, used in the Rijndael encryption algorithm, is considered to be strong.

The growth of calculating power of the computer necessitates an increase of the cryptographic strength of encryption algorithms.

The authors have proposed substitution blocks for each round of the Rijndael scheme, based on different irreducible polynomials. A study of compositions representing a different combination of specially selected irreducible polynomials for ten rounds was carried out and the optimal set of polynomials with the best values of the encryption quality indicators by the Rijndael scheme was obtained.

Keywords: replacement blocks, GOST, Rijndael, boolean function, block encryption algorithms, cryptographic stability.

СОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ КОНСТРУИРОВАНИЯ БЛОКОВ ЗАМЕН ДЛЯ АЛГОРИТМОВ СИММЕТРИЧНОГО ШИФРОВАНИЯ

А. С. Меринов, К. А. Нестеров, О. Н. Жданов*

Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева
Российская Федерация, 660037, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31
*E-mail: onzhdanov@mail.ru

Как известно, для обеспечения конфиденциальности информации широко применяются блочные симметричные алгоритмы шифрования. Стойкость алгоритмов шифрования к наиболее распространенным видам криптоанализа во многом определяется качеством блока замен.

В настоящей работе продолжается разработка методики построения блоков замен.

При первом подходе в качестве компонентных функций блоков замен используются булевы функции, обладающие заданными криптографическими свойствами. Ранее одним из авторов была предложена обоснованная методика поэтапного выбора булевых функций для конструирования блоков. Однако эта методика учитывала только расстояние нелинейности первого порядка.

В данной работе, помимо таких криптографических свойств булевых функций, как сбалансированность, обладание строгим лавинным эффектом, обладание корреляционным иммунитетом, впервые одновременно рассматриваются расстояния нелинейности первого и второго порядков булевых функций.

Проведено исследование полного множества булевых функций от четырех переменных, результатом которого является оптимальный набор булевых функций для построения блоков замен при шифровании алгоритмом ГОСТ 28147–89.

При втором подходе блок замены определяется неприводимым полиномом над полем Галуа. Такая схема применена в считающемся стойким алгоритме шифрования Rijndael.

Рост вычислительной мощности ЭВМ обуславливает необходимость увеличения криптостойкости алгоритмов шифрования.

Авторами предложены блоки замен для каждого раунда схемы Rijndael, основанные на различных неприводимых полиномах. Проведено исследование композиций, представляющих собой различное сочетание специально подобранных неприводимых полиномов в десяти раундах, что позволило выбрать оптимальное множество многочленов с наилучшими значениями показателей качества шифрования по схеме Rijndael.

Ключевые слова: блоки замен, ГОСТ, Rijndael, булевы функции, алгоритмы блочного шифрования, криптографическая стойкость.

Introduction. As it is known, block symmetric encryption algorithms are widely used to ensure confidentiality. The growth of computer processing power and the development of cryptanalysis methods require increasing the cryptographic stability of existing algorithms and the development of new ones. Researchers and practitioners are conducting work in this direction. The stability of the encryption algorithm to the most common types of cryptanalysis is determined by the quality of the replacement block, the substitution block. At present, it is already generally accepted that the quality of replacement units is characterized by the values of nonlinearity and avalanche effect [1; 2].

There are two main approaches to the construction of replacement tables.

Thus, in [3], a reasonable method was proposed for the step-by-step selection of Boolean functions that are components of the replacement block, which takes into account not only the nonlinearity of each of the functions making up the block, but also the nonlinearity of all possible nontrivial linear combinations. It is also noted that it is possible to simultaneously solve the problem of increasing stability, both to linear and differential cryptanalysis methods, if both nonlinearity and dynamic distance are used as selection criteria [4–6]. The methodology of step-by-step selection was programmatically implemented in relation to the algorithm of GOST 28147–89, currently considered to be very stable, in [1].

The most typical example of the second approach is also the Rijndael algorithm [7], which is considered to be stable, in which the replacement block is completely determined by an irreducible polynomial over the Galois field. In Rijndael the construction of Nyberg is used [8], which is a reflection in the form of multiplicatively inverse elements of the Galois field $GF(2^k)$:

$$y = x^{-1}\,\mathrm{modd}[f(z), p], \quad y, x \in GF(2^k)\,, \tag{1}$$

in combination with affine transformation:

$$b = A \cdot y + a, \quad a, b \in GF(2^k)\,, \tag{2}$$

where $f(z) = z^8 + z^4 + z^2 + z + 1$ – irreducible over the field $GF(2^8)$ polynomial; A – non-degenerate affine transformation matrix; a – shift vector; $p = 2$ – characteristic of the extended Galois field, $0^{-1} \equiv 0$ – by definition; a, b, x, y – elements of the extended Galois field $GF(2^k)$, which are considered as decimal numbers, or binary vectors, or polynomials of degree $k-1$.

Among the quality indicators of S-units, the following are most often distinguished [2]:

– maximum of the modules of the matrix elements of the correlation coefficients of the input and output bits;

– the number of zeros in the matrix of correlation coefficients;

– non-linearity, understood as the distance to the set of affine functions;

– algebraic degree of nonlinearity.

It is noted that the S-blocks of the Nyberg construction have many practically valuable cryptographic properties, such as high nonlinearity distance, homogeneous minimization of correlation coefficients, and relative simplicity of technical implementation both using the tabular method and using Galois field operations.

In the present work, research is continued in these two directions.

The study of the set of Boolean functions of four variables. The study of the full set of Boolean functions of four variables was carried out. In addition to cryptographic properties of Boolean functions, such as: balance, possessing a strict avalanche effect, possessing correlation immunity, for the first time the nonlinearity distances of the first and second orders of Boolean functions are simultaneously considered.

Nonlinearity of r- order $nl_r(f)$ of Boolean function f over F_2^n is called $\min\limits_{\deg(l) \le r} d(f, l)$. Nonlinearity $nl_1(f)$ of Boolean function f is called the distance between f and a set of affine functions. Nonlinearity $nl_2(f)$ of Boolean function f is called the distance between f and a set of quadratic functions.

For example, a Boolean function of four variables with the following truth table:

$f=\{000101001001101\}$, its nonlinearity of the first order is 3 and the nonlinearity of the second order is 1.

The result of the study of the nonlinearity of the first and second orders Boolean functions of four variables is presented in tab. 1.

Table 1

Nonlinearity of the first and second orders of Boolean functions

Nonlinearity distance		Class scopes
1 order	2 order	
0	0	22
1	1	0
2	2	0
3	1	0
4	0	200
4	2	0
5	1	0
6	0	0

So, there are a total of 22 linear first-order Boolean functions and 200 second-order linear Boolean functions with these characteristics. Boolean functions with a first order nonlinearity distance equal to 0 will not be considered further, since the replacement blocks obtained from them are unstable to linear cryptanalysis [9].

The remaining 200 Boolean functions are linear functions of the second order, they are not enough to study the nonlinearity of higher orders. Therefore, Boolean functions not linear of the first and second orders were found, and the maximum value of the correlation coefficient of the replacement block when using these functions at absolute value was minimal.

The correlation properties of the substitution units were analyzed; Boolean functions with the same nonlinearity properties of the first and second orders were used as component functions. The results of the study are shown in tab. 2, which reflects the maximum correlation coefficient of the replacement unit in absolute value when using certain Boolean functions and the number of such functions.

Boolean functions with a first order nonlinearity distance equal to 1, 3, 5, and 6 are not balanced Boolean functions because they cannot be used as component functions of the replacement blocks of the encryption algorithm. Bijective replacement units with a maximum correlation coefficient of 0.25 were worked out, using Boolean functions with the following properties:

– the first order nonlinearity distance is 4;
– the second order nonlinearity distance is 2;
– balance;
– have a strict avalanche effect.

Bijective replacement blocks with a maximum correlation coefficient of 0.25 were constructed, using Boolean functions with the following properties:

– the first-order nonlinearity distance is 2;
– the second-order nonlinearity distance is 2;
– balance.

Table 2

Class volumes

Nonlinearity distance		The maximum modulus of the correlation coefficient of a bijective replacement block	Class volume s
1 order	2 order		
0	0	0	22
1	1	Doesn’t exist	0
2	2	0.25	1408
3	1	Doesn’t exist	0
4	0	0	304
4	2	0.25	5280
5	1	Doesn’t exist	0
6	0	Doesn’t exist	0

These Boolean functions do not satisfy the strict avalanche criterion; therefore, replacement blocks obtained from such Boolean functions are less resistant to the differential cryptanalysis method.

We distinguish two sets of Boolean functions that are most suitable to construct blocks of replacement.

For testing, the AES encryption algorithm was chosen and the following tests were used: series distribution, autocorrelation function, D. Knuth's correlation test:

– the first order nonlinearity distance is 4;
– the second-order nonlinearity distance is 2;
– balance;
– have a strict avalanche effect.

The power of the recieved set is 5280. The functions of this set can be recommended for use as a component of replacement blocks for the algorithms of GOST 28147-89, AES and (with minor and obvious changes) of similar algorithms.

The set of boolean functions used to build the replacement block is shown below. The test results presented in fig. 1–3, indicate the quality of the constructed replacement unit.

$$F=[0,0,0,0,0,1,1,1,0,1,1,1,0,1,1,0];$$

$$F=[0,0,0,0,1,0,1,1,1,0,1,1,1,0,0,1];$$

$$F=[0,0,1,1,1,1,0,1,0,0,0,1,1,0,1,0];$$

$$F=[1,0,1,0,0,1,0,0,1,0,1,1,1,1,0,0].$$

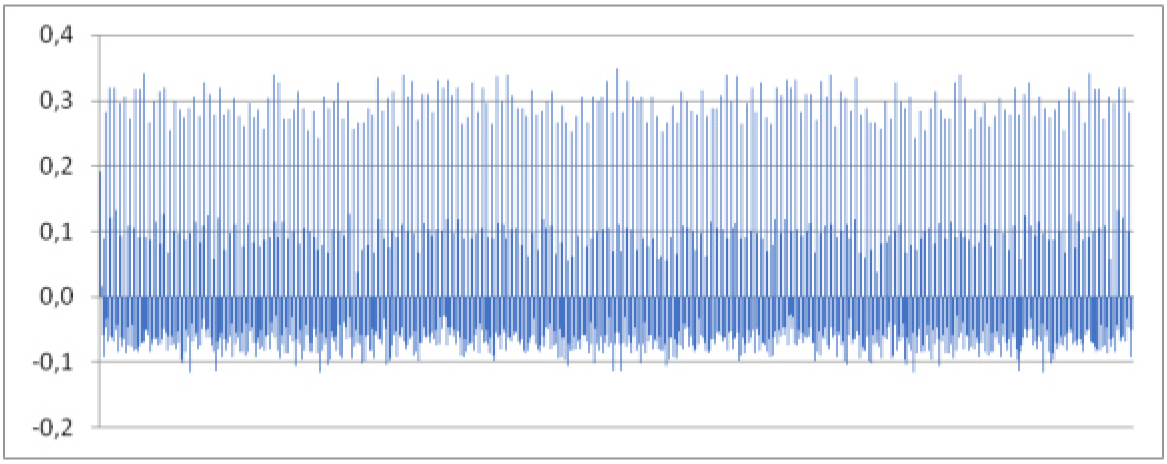

Fig. 1. Autocorrelation function

Рис. 1. Автокорреляционная функция

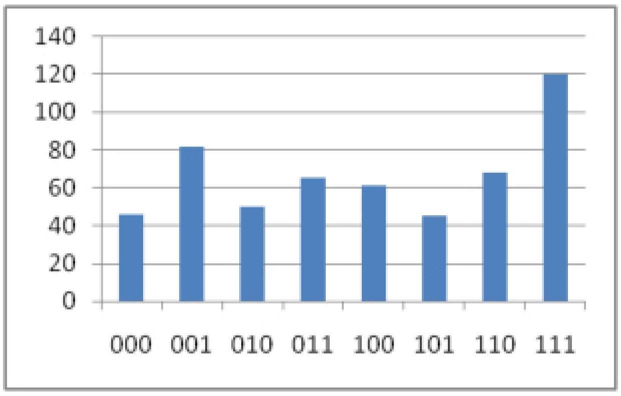

Fig. 2. Schedule distribution of series-triples

Рис. 2. График распределения серий троек

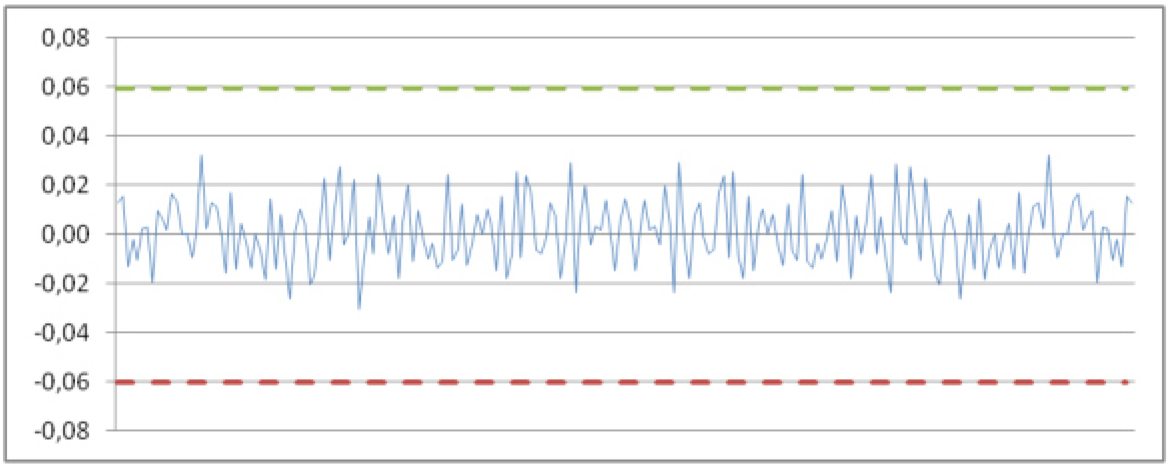

Fig. 3. The result of D. Knut's correlation test

Рис. 3. Результат проверки корреляции Д. Кнута

Selection of optimal irreducible polynomials for the implementation of the AES algorithm. One of the techniques for enhancing the durability of the AES algorithm is the construction of replacement blocks based not on one selected irreducible polynomial for all rounds, but on various irreducible polynomials chosen for each round. However, due to unacceptable computational complexity (10^{10} combinations), first it was decided to conduct a study of compositions, which are a different combination of five specially selected irreducible polynomials in ten rounds.

In works [10; 11], nonlinear transformations of the Nyberg construction were studied in detail on the basis of all isomorphic and automorphic representations of the fields. All irreducible polynomials over the fields are presented, and the values of the quality indicators determined by these S-blocks polynomials are calculated. The possibility of choosing one of the many irreducible polynomials is of practical importance.

After the publication of papers [5; 6; 10], it became possible to combine the advantages of the GOST and Rijndael approaches.

In article [11] the use of irreducible polynomial compositions is analyzed. The composition in this case is the alternation of two irreducible polynomials. Irreducible polynomials, with the most remarkable cryptographic characteristics, were taken from this article. Encryption was carried out using each of the polynomials on 20 texts (the same polynomial was used in each round).

As a result, cryptographic characteristics were obtained and a comparative analysis of indicators for each irreducible polynomial was carried out (tab. 3, 4). Polynomials are represented by their decimal equivalents, and filled cells show the most remarkable indicators for each irreducible polynomial.

As a result, irreducible polynomials were selected – 283, 319, 333, 355, 357, since they have minimum values of the maximum modulus of the correlation coefficients and the largest number of zero elements of the correlation matrix.

Then an encryption procedure was carried out with all possible combinations of selected irreducible polynomials and five open texts.

Using the same encryption quality criteria, the maximum of the modules of the matrix coefficients correlation elements and the number of zeros of the elements of the correlation matrix, correlation matrices were constructed and a comparative analysis of indicators for each composition was performed. The selection of the best compositions of irreducible polynomials, surpassing the rest of the compositions in cryptographic characteristics, was done.

Table 3

The maximum modulus of the correlation coefficients

№ text	Maximum of the modules of the correlation matrix elements									
	Irreducible polynomials									
	283	285	299	301	313	319	333	351	355	357
1	0.75	0.75	0.625	0.625	0.625	0.5	0.5	0.625	0.5	0.5
2	0.5	0.5	0.625	0.75	0.625	0.5	0.5	0.5	0.5	0.625
3	0.5	0.875	0.625	0.5	0.625	0.5	0.5	0.5	0.75	0.625
4	0.5	0.5	0.5	0.5	0.625	0.5	0.625	0.625	0.75	0.5
5	0.625	0.625	0.625	0.75	0.5	0.75	0.625	0.625	0.625	0.5
6	0.75	0.75	0.625	0.625	0.5	0.5	0.5	0.5	0.625	0.5
7	0.5	0.625	0.75	0.625	0.625	0.75	0.625	0.625	0.5	0.625
8	0.625	0.625	0.5	0.5	0.5	0.625	0.625	0.75	0.625	0.5
9	0.5	0.625	0.625	0.5	0.625	0.625	0.5	0.625	0.5	0.5
10	0.5	0.625	0.625	0.625	0.625	0.625	0.625	0.75	0.75	0.75
11	0.5	0.625	0.625	0.75	0.375	0.5	0.625	0.625	0.5	0.5
12	0.75	0.5	0.625	0.625	0.625	0.5	0.5	0.5	0.625	0.625
13	0.5	0.5	0.75	0.625	0.75	0.5	0.625	0.625	0.5	0.5
14	0.625	0.75	0.625	0.625	0.5	0.625	0.625	0.625	0.625	0.5
15	0.625	0.5	0.625	0.625	0.625	0.875	0.75	0.625	0.625	0.5
16	0.625	0.5	0.75	0.625	0.5	0.5	0.625	0.625	0.625	0.625
17	0.5	0.625	0.75	0.625	0.75	0.625	0.625	0.5	0.625	0.625
18	0.625	0.75	0.625	0.625	0.625	0.5	0.75	0.5	0.5	0.75
19	0.625	0.625	0.625	0.5	0.5	0.5	0.5	0.625	0.375	0.5
20	0.625	0.625	0.625	0.625	0.5	0.75	0.5	0.5	0.5	0.5

Table 4

The number of zeroes of the correlation matrix elements

№ text	The number of zeros of the correlation matrix									
	Irreducible polynomials									
	283	285	299	301	313	319	333	351	355	357
1	9	13	10	15	9	15	10	9	9	14
2	16	11	9	12	16	19	18	18	15	11
3	10	9	12	10	13	15	14	15	13	13
4	13	11	12	7	12	16	7	16	18	14
5	19	19	11	11	7	19	8	8	3	21
6	8	14	11	11	16	15	9	15	11	11
7	10	20	16	12	7	11	23	4	14	12
8	12	15	19	13	11	9	9	13	16	7
9	9	15	8	9	13	14	15	14	12	14
10	12	13	14	14	17	12	19	17	13	11
11	21	11	12	10	12	12	15	13	11	14
12	20	13	13	21	10	9	6	18	11	6
13	10	9	11	13	19	18	9	17	14	12
14	7	9	10	21	19	17	10	13	13	7
15	8	10	9	17	8	19	10	7	9	4
16	16	14	11	15	13	15	9	13	13	16
17	14	12	6	13	10	13	13	13	10	12
18	16	11	14	18	9	9	13	12	11	10
19	16	13	7	10	17	10	14	13	13	17
20	10	17	10	16	12	9	9	13	15	13

The composition here is a combination of five polynomials in ten rounds. For example, compositions 333, 283, 283, 319, 357, 283, 333, 355, 283, 333 (or 2001402302). Experiments have shown that the use of the listed irreducible polynomials in Rijndael encryption provides the best cryptographic strength indicators in comparison with others. Examples of the best and the worst compositions on two criteria are presented respectively in tab. 5, 6.

Table 5

Examples of the best compositions on the basis of two criteria

Maximum correlation coefficient	Number of zeroes	Composition
0.375	36	3104034331
0.375	34	3313210233
0.375	34	4142344410
0.375	34	4303234230
0.375	33	4202203343
0.375	33	4324342340
0.375	32	333434303
0.375	32	2422044342
0.375	32	4443342101
0.25	30	3241333141

Table 6

Examples of the worst compositions on the basis of two criteria

Maximum correlation coefficient	Number of zeroes	Composition
0.625	7	32000000003
0.75	9	32000000004
0.625	16	32000000140
0.875	11	32112010432
0.625	11	32112010433
0.75	12	32000000143
0.875	16	32000000222
0.625	13	32201110444
0.75	11	32201111000
0.875	14	32000001120

The data in the tab. 5 are not fully presented, since the output of all data would take several hundred pages, and their information content would tend to zero. The program, which is engaged in the calculation of the above data, can be found by clicking the following link [12].

The compositions presented in tab. 5, have high rates of cryptographic characteristics. The results of the study allow choosing the optimal set of polynomials with the best cryptographic properties, the combination of which gives a high rating of the quality of encryption according to the AES scheme, which increases the cryptographic strength of the AES algorithm.

The developed method allows selecting encryption options in such a way that it can compete not only with the standard AES encryption algorithm, but also with other modern block encryption algorithms.

Conclusion. The results of the study of two approaches showed a good quality of substitution units construction, which ensures the best cryptographic performance indicators, both for the Rijndael algorithm and for GOST. On the basis of the obtained results, it is necessary to further explore possible options of increasing the strength of block encryption algorithms. It is interesting to compare the obtained results with their ternary counterparts, see [13].

Acknowledgment. The authors express their gratitude to Sokolov Artem Viktorovich.

Благодарности. Авторы выражают благодарность Соколову Артему Викторовичу.

References

1. Zhdanov O. N. *Metodica vibora kluchevoi informacii dla algoritmov blochnoigo shifrovania* [The method of selecting key information for the block cipher algorithm]. Moscow, INFRA-M Publ., 2013, 97 p.

2. Sokolov A. V. New methods for synthesizing nonlinear transformations of modern ciphers. Germany, Lap Lambert Academic Publishing, 2015, 100 p.

3. Mister S., Adams C. Practical S-box design. Workshop in selected areas of cryptography. SAC'96, 1996, P. 61–76.

4. Medvedeva T. E. [Evaluation of the cryptographic stability of the replacement tables of the algorithm State Standard 28147-89]. *Reshetnevskie chteniya.* 2012, Vol. 2, No.15, P. 66–667 (In Russ.).

5. Chalkin T. A., Zolotuchin V. U. [Development of a methodology for selecting parameters for the algorithm for constructing replacement nodes of the block cipher GOST 28147-89]. *Prikladnaya diskretnaya matematika. Prilozhenie.* 2010, No. 3, P. 20–21 (In Russ.)

6. FIPS 197. Advanced encryption standard. Available at: http://csrc.nist.gov/publications (accessed 10.10.2018).

7. Nyberg K. Differentially uniform mappings for cryptography. Advances in cryptology. Proc. of EUROCRYPT'93, Lecture Notes in Compuer Springer Verlag. Berlin, Heidelberg, New York, 1994, P. 55–65.

8. Mazurkov M. I., Sokolov A. V. [Nonlinear transformations on the basis of complete classes of isomorphic and automorphic representations of the field GF(256)]. *Izvestiya vuzov.* Vol. 56, No. 11 (In Russ.). Doi: https://doi.org/10.20535/S0021347013110022.

9. Agafanov I. V. *Kriptograficheskie svoystva nelineynykh bulevykh funktsiy* [Cryptographic properties of nonlinear boolean functions]. St. Petersburg, DHA&CAGD Publ., 2007, P. 1–24.

10. Mazurkov M. I., Sokolov A. V. [Cryptographic properties of the nonlinear transformation of the cipher Rijndael on the basis of complete classes of irreducible polynomials]. *Trudy Odesskogo politekhnicheskogo universiteta*. 2012. No. 2(39), P. 183–18.

11. Dmitriev M. A. [Possible options for increasing the cryptographic strength of encryption algorithms based on the Nyberg design]. *Siberian Journal of Science and Technology.* 2017, Vol. 18, No. 3, P. 505–503 (In Russ.).

12. Merinov A. S. The program that performs the encryption procedure by the method of selecting the optimal parameters for the implementation of the AES algorithm. Available at: https://yadi.sk/d/PrPh5I1E3WfwBz (accessed 9.10.2018).

13. Zhdanov O. N., Sokolov A. V. [Extending Nyberg construction on Galois fields of odd characteristic]. *Izvestiya vuzov. Radioelektronika.* 2017, Vol. 60, No. 12, P. 696–702 (In Russ.).

14. *GOST 28147–89. Sistemy obrabotki informatsii. Zashchita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovaniya* [State Standard 28147–89. Information processing system. Cryptographic protection. Algorithm of cryptographic transformation]. Moscow, Standartinform Publ., 1996. 28 c.

15. Report on the Development of the Advanced Encryption Standard (AES) Available at: https://nvlpubs.nist.gov/nistpubs/jres/106/3/j63nec.pdf (accessed 11.10.2018).

Библиографические ссылки

1. Жданов О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования. М. : Инфра-М, 2013. 97 с.

2. Соколов А. В. Новые методы синтеза нелинейных преобразований современных шифров. Германия. Саарбрюккен : Lambert Academic Publishing, 2015. 172 с.

3. Mister S., Adams C. Practical S-box design. Workshop in selected areas of cryptography. SAC'96. P. 61–76.

4. Медведева Т. Е. Оценка криптостойкости таблиц замен алгоритма ГОСТ 28147–89 // Решетневские чтения. 2012. Т. 2, № 15. С. 66–667.

5. Чалкин Т. А. Золотухин В. Ю. Разработка методики оценки зависимости криптостойкости алгоритма ГОСТ 28147–89 от выбранной ключевой информации // Прикладная дискретная математика. Приложение. 2010. № 3. С. 20–21.

6. FIPS 197. Advanced encryption standard [Электронный ресурс]. URL: http://csrc.nist.gov/ publications (дата обращения: 10.10.2018).

7. Nyberg K. Differentially uniform mappings for cryptography // Proc. of EUROCRYPT'93, Lecture Notes in Compuer Springer Verlag. Berlin, Heidelberg, New York, 1994. P. 55–65.

8. Мазурков М. И., Соколов А. В. Нелинейные преобразования на основе полных классов изоморфных и автоморфных представлений поля GF(256) // Известия вузов. Т. 56, № 11. Doi: https://doi.org/10.20535/S0021347013110022.

9. Агафонова И. В. Криптографические свойства нелинейных булевых функций. СПб. : DHA & CAGD, 2007. С. 1–24.

10. Мазурков М. И. Криптографические свойства нелинейного преобразования шифра Rijndael на базе полных классов неприводимых полиномов // Труды Одесского политехнического университета. 2012. Вып. 2(39). С. 183–18.

11. Дмитриев М. А. Возможные варианты повышения криптостойкости алгоритмов шифрования на основе конструкции Ниберг // Сибирский журнал науки и технологий. 2017. Т. 18, № 3. С. 505–509.

12. Merinov A. S. The program that performs the encryption procedure by the method of selecting the optimal parameters for the implementation of the AES algorithm [Электронный ресурс]. URL: https://yadi.sk/d/PrPh5I1E3WfwBz (дата обращения: 9.10.2018).

13. Жданов О. Н., Соколов А. В. О распространении конструкции Ниберг на поля Галуа нечетной характеристики // Известия вузов. Радиоэлектроника. 2017. Т. 60, № 12. С. 696–702.

14. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М. : Стандартинформ, 1996. 28 с.

15. Report on the Development of the Advanced Encryption Standard (AES) [Электронный ресурс] URL: https://nvlpubs.nist.gov/nistpubs/jres/106/3/j63nec.pdf (дата обращения: 11.10.2018).

Merinov Alexander Stanislavovich – Master student of the Department of Information Technology Security; Reshetnev Siberian State University of Science and Technology. E-mail: onzhdanov@mail.ru.

Nesterov Kirill Alexandrovich – Master student of the Department of Information Technology Security; Reshetnev Siberian State University of Science and Technology. E-mail: onzhdanov@mail.ru.

Zhdanov Oleg Nikolayevich – Cand. Sc., Associate Professor of the Department of Information Technology Security; Reshetnev Siberian State University of Science and Technology. E-mail: onzhdanov@mail.ru.

Меринов Александр Станиславович – магистрант; кафедра безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева. E-mail: onzhdanov@mail.ru.

Нестеров Кирилл Александрович – магистрант; кафедра безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева. E-mail: onzhdanov@mail.ru.

Жданов Олег Николаевич – кандидат физико-математических наук, доцент; кафедра безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева. E-mail: onzhdanov@mail.ru.